

Policy:

FIN 008 Security

Executive or Associate Director lead	Executive Director of Finance
Policy author/lead	Security and Fire Officer
Feedback on implementation to	Security and Fire Officer

Document type	Policy
Document status	Version 7
Date of initial draft	July 2018
Date of consultation	4th - 31st July 2018
Date of verification	10 December 2018
Dates of ratification	20 December 2018
Ratified by	Executive Directors' Group
Date of issue	21 December 2018
Date for review	Review process, (including re-ratification), to be scheduled for completion within 3 years of the previous ratification date

Target audience	All SHSC staff and the Trust Board
Keywords	

Security Policy: Version 7

This policy is stored and available through the Sheffield Health and Social Care (SHSC) NHS Foundation Trust's intranet and internet.

This version of the policy supersedes the previous version, (V6 October 2015). All copies of the previous policy held separately should be destroyed and replaced with this version.

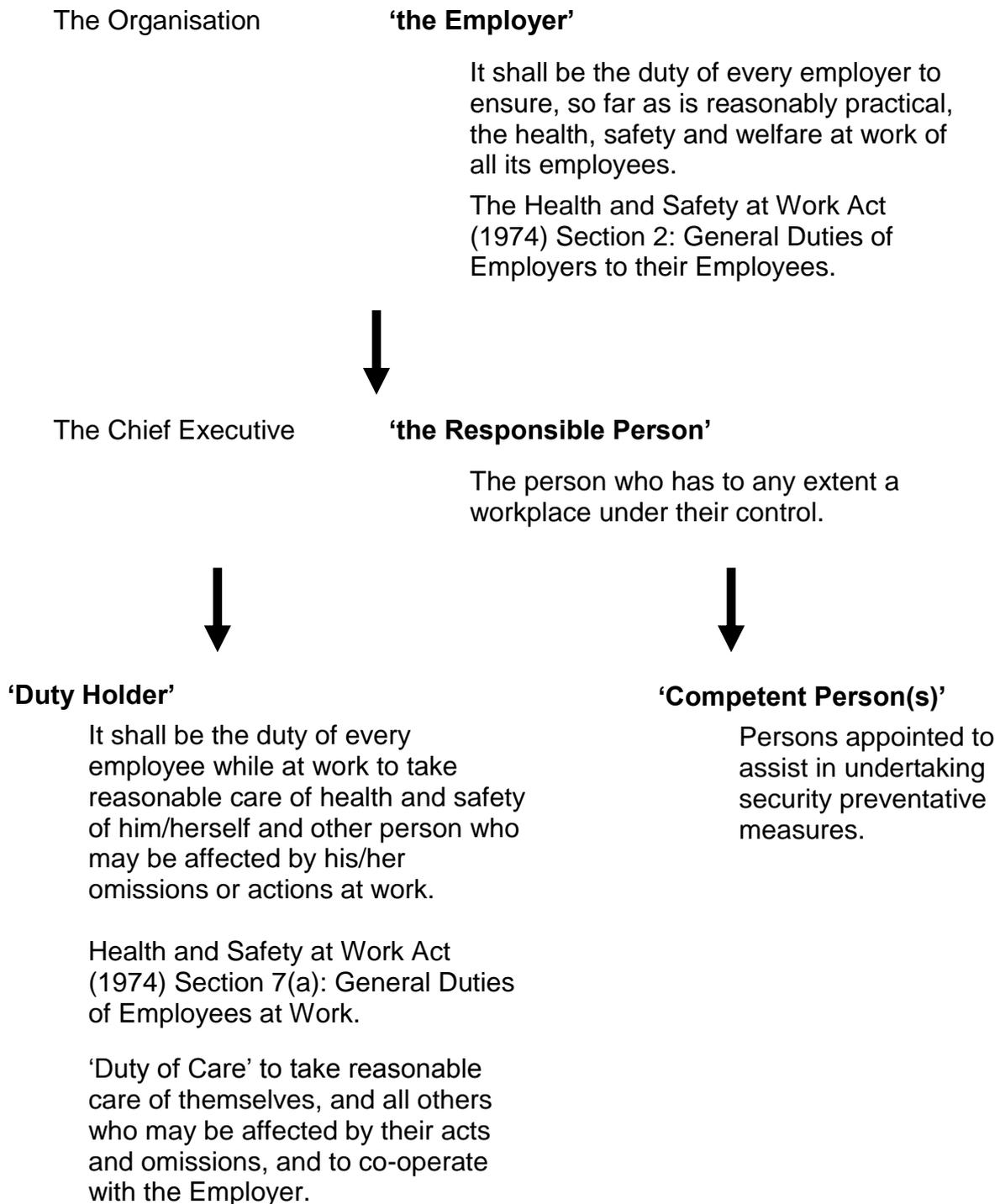
Contents

Section		Page
	Flowchart	
1.	Introduction	1-2
2.	Scope	2-3
3.	Definitions	3
4.	Purpose	3-4
5.	Duties	4
	Trust Board (Board of Directors)	4
	Executive Directors Group (EDG)	4
	Scheme of Delegation	4
	Chief Executive	4
	Security Management Director (SMD)	4
	Security Officer	4
	Director of Finance	4
	Head of Procurement	5
	Emergency Planning Manager	5
	Director of Human Resources	5
	Chief Pharmacist	5
	Clinical and Service Directors and Directors of Corporate Functions	5
	Director of Facilities	5
	Head of Estate Services	5
	Head of Capital and Strategic Development Managers	5
	Staff	6
	6.	Process
6.1 Identifying Risks		6
6.2 Assessing Risks		6
6.3 Risk Management and Action Plans		6
6.4 Risk Review		6
6.5 Reporting Incidents and Serious Incidents		7
6.6 Protection of Staff - Tackling Aggression and Violence		7
6.7 Security and Management of Assets and Property		7
6.8 Investigations, Sanctions and Publication		8
6.9 Recovering Financial Losses		8
6.10 Major Incident and Contingencies - Lockdown		8
6.11 Medicines, Drugs, Prescription Forms and Hazardous Materials		9
6.12 Counter-terrorism		9
6.13 Lone Working		9
6.14 Dangerous and 'Offensive' Weapons		10

7.	Dissemination, storage and archiving	10
8.	Training and other resource implications	11
9.	Audit, monitoring and review	11
10.	Implementation plan	12
11.	Links to other policies, standards and legislation	12
12.	Contact details	13
13.	References	13
Appendices	Appendix A Version control and amendment log	14
	Appendix B Dissemination record	15
	Appendix C Equality impact assessment form	16
	Appendix D Human Rights Act assessment checklist	17-18
	Appendix E Development, consultation and verification record	19-21
	Appendix F Policy checklist	22-23

Flowchart:

Management Structure for Security



1. Introduction

This document explains the strategic approach Sheffield Health and Social Care NHS Foundation Trust, (SHSC), will take to provide a safe and secure physical environment that has suitable systems and arrangements in place to protect staff from violence, harassment and abuse; safeguard property and assets from theft, misappropriation or criminal damage.

The Trust will deliver a security strategy designed to meet the aims of the document through its governance structure by addressing the priority areas:

- Creating a pro-security culture

The Trust will, through its governance structure, allow for the creation of a pro-security culture whereby staff are supported and encouraged to effectively manage security arrangements within their workplace and report any security incidents, including theft, un-authorised access, violence and other unacceptable practices when they occur.

The Trust will provide Security Awareness Training to all staff during corporate and local workplace induction. Line managers will explain security systems and arrangements applicable to members of staff and the support systems available, if required.

- Deterrence

The Trust will implement appropriate, protective measures including physical and psychological barriers to deter or delay criminal activities. The purpose of deterrence methods is to convince potential attackers that a successful attack is unlikely due to strong, external and internal defences.

Physical measures to protect work premises, including walls, fencing, intrusion detection systems, restricted access points, warning signs and security lighting will be considered by Trust employees during design, planning, construction and refurbishment of premises.

Measures employed will serve to prevent, or at least delay attacks and act as a psychological deterrent by defining the perimeter of the premise and making un-authorised intrusions more difficult.

- Preventing

Where possible, the Trust will develop appropriate procedural arrangements to prevent security incidents or breaches from occurring in the first instance, or minimise the risk of them occurring, learning from operational experience and shared best practice. Staff and authorised persons will be provided with suitable means of identification, i.e. identity cards. All staff are required to either display, or have in their immediate possession, their approved identity card as a deterrent to prevent avoidable breaches in security provisions.

- Detecting

All Trust premises will be provided with suitable electronic and/or physical security systems to detect breaches in security provisions. Staff are required to be vigilant and conscious of persons acting suspiciously within Trust premises and not displaying approved personal identification. They are to report any incident immediately to a senior member of staff or Police, (if deemed appropriate).

- Investigating

All breaches in security are to be investigated by line-management in accordance with the Trust's governance arrangements.

Investigations are to be undertaken in a fair, objective and professional manner to ensure those responsible for such incidents are held to account for their actions. Where it is considered that redress is required to be taken against individuals responsible for causing, injury, harm, fear or damage to staff, service users or organisational assets, support and assistance is available from the Trust's Security Officer and Police.

Increased Security Threats

Following the identification of an increased security threat, additional resources may be allocated to mitigate, where considered appropriate. Where it is considered that a security service is required, which cannot be provided internally by staff, approved external contractors will be appointed. All external, security contractors are to be commissioned via the Facilities Directorate.

2. Scope

This policy applies to:

- All premises and property owned- or leased by SHSC;
- Staff employed by SHSC, (full-time and part-time employees);
- Visitors;
- Contractors;
- Sub-contractors;
- Students;
- Volunteers;
- All other persons engaged in business on behalf of SHSC.

Responsibility for the management of this policy will be devolved in accordance with the organisation's devolved management structure, which includes aspects of crime prevention. The responsibility of operational managers is to ensure procedural arrangements within their sphere of responsibility are devised and implemented, taking account of security issues and that staff groups for which they have responsibility receive appropriate training.

The day-to-day management of security issues will remain the responsibility of operational managers. SHSC will appoint a Security Officer who will act in an advisory capacity to support staff to enable them to discharge their responsibilities.

SHSC, through its devolved governance structure, will ensure appropriate security measures are identified with control measures implemented to protect, detect and respond to security risks which are considered to pose a significant risk to service provision.

3. **Definitions**

An explanation of terms used within this policy is provided below:

Physical assault - the intentional application of force to a person without lawful justification; resulting in physical injury or personal discomfort.

Non-physical assault - the use of inappropriate word(s) or behaviour causing distress and/or constituting harassment.

Work-related violence - (Health and Safety Executive (HSE) definition) - any incident in which a person is abused, threatened or assaulted in circumstances relating to their work.

Duty of care - (Health and Safety at Work Act (1974) Section 7) - it shall be the duty of every employee whilst at work:

- To take reasonable care for the health and safety of his/herself and of other persons who may be affected by his/her acts or omissions at work;
- As regards any duty or requirement imposed on his/her employer, or any other person, by or under any of the relevant statutory provisions, to co-operate with him/her, so far as is necessary, to enable that duty or requirement to be performed or complied with.

4. **Purpose**

It is this policy's intention to enable management teams and staff groups to ensure the delivery of healthcare takes place in a safe and secure environment, free from the risks of criminal activity which may arise when providing a public service.

To achieve the intended function, the purpose of this policy is to:

- Identify persons with responsibility for security management;
- Identify security risks;
- Ensure effective risk management processes are implemented to remove/reduce security risks;
- Ensure security risks recorded at all levels of the organisation are appropriately managed;
- To establish a safe and secure environment that has systems, policies and other arrangements to protect staff from violence, harassment and abuse; safeguard property and assets from theft, and criminal damage..

This policy outlines how SHSC will provide the best possible protection for its staff, service users, property and assets.

SHSC will ensure, wherever possible, that sufficient resources and governance arrangements are provided to facilitate a properly secure environment.

This document outlines the measures SHSC will undertake in seeking to raise security management standards.

5. Duties

All staff have a duty of care to ensure all reasonable measures are undertaken to protect Trust property, equipment and minimise the risk of injury and/or harm to staff, service users, visitors and other relevant persons. This duty is applicable to staff who are seconded to, or work in, Trust services through service level agreements and SHSC staff working in other NHS Trusts or services.

Trust Board (Board of Directors)

The Board is responsible for ensuring:

- Effective financial stewardship through value for money, financial control and financial planning and strategy;
- High standards of corporate governance are maintained in the conduct of the business of the Trust.

Executive Directors Group (EDG)

EDG is responsible for ensuring the operational delivery of the Trust's strategic direction.

Scheme of Delegation

The Trust may make such arrangements, as considered appropriate, to ensure its functions are implemented by a committee, sub-committee, the Chairman, a director or by an officer of the Trust; in each case subject to such restrictions and conditions as the Board deems suitable in accordance with the Trust's Scheme of Delegation Policy.

Chief Executive

The Chief Executive has overall responsibility for security within SHSC and will appoint an appropriate Executive Director to undertake the role of Security Management Director.

Security Management Director (SMD)

The SMD is responsible for overseeing and providing strategic management and support for all security management work within the Trust.

Security and Fire Officer

The Security and Fire Officer is to advise and assist employees in matters of security within the workplace.

Director of Finance

The Director of Finance is responsible for Trust policy documents: *Standing Orders, Reservations and Delegation of Powers and Standing Financial*, and *Scheme of Delegation*, ensuring their contents are strictly observed and enforced and suitable arrangements are established.

Head of Procurement

The Head of Procurement will ensure all purchases are made in accordance with the Trust document: *Standing Orders, Reservations and Delegation of Powers and Standing Financial Instructions*.

Emergency Planning Manager

The Emergency Planning Manager is responsible for ensuring the Trust has suitable arrangements for the event of a major incident and that detailed guidance on actions to be undertaken in such circumstances is contained within the policy *Emergency Preparedness, Resilience and Response (EPRR)*.

Director of Human Resources

The Director of Human Resources is responsible for ensuring security-related issues are addressed within the SHSC personnel policies and implementation of the government's 'PREVENT' programme, which aims to support, protect and safeguard the Trust's staff and service users.

Chief Pharmacist

The Chief Pharmacist is responsible for medicines management throughout the Trust, including effective governance and security arrangements for the safe management of medicines. The Chief Pharmacist Associate is the Trust's 'Accountable Officer for Controlled Drugs' and is responsible for the assurance of governance relating to controlled drugs.

Clinical and Service Directors and Directors of Corporate Functions

Clinical and Service Directors, and Directors of Corporate Functions, are responsible for ensuring suitable governance arrangements are brought to the attention of staff and implemented within all areas where they have devolved responsibility.

Director of Facilities

The Director of Facilities is responsible for the development of secure facilities as directed by the Trust Board and for devolving responsibility to appropriate persons to plan, design and maintain the security of Trust premises.

Head of Estate Services

The Head of Estate Services is responsible for ensuring appropriate advice, technical support and control measures are provided by suitably-qualified persons for the monitoring, installation and maintenance of security measures within Trust premises.

Head of Capital and Strategic Development

The Head of Capital and Strategic Development is responsible for ensuring a secure environment is considered at the briefing, planning, design and construction stages of all new-build or refurbishment projects using a risk-based approach.

Managers

Managers with devolved responsibilities are to ensure all reasonable and practical measures are undertaken to identify, evaluate and mitigate security risks.

Staff

All staff have a responsibility to comply with authorised instructions and management arrangements, which have been devised to provide a safe and secure environment.

6. Process

The following processes have been devised to mitigate risk, where appropriate.

6.1 Identifying Risks

The person(s) delegated with responsibility for workplace activities must manage the health and safety of staff, and other relevant persons for whom they have responsibility, in accordance with the *Health and Safety at Work Act 1974*.

In addition, they must undertake workplace risk assessments, and record significant risks, in accordance with the *Management of Health and Safety at Work Regulations 1999* and the Trust's *Health and Safety Policy*.

The Trust has an effective *Risk Management Strategy*, which describes the processes for effectively managing risks within the Trust.

Potential hazards and risks likely to affect security management - especially those health and safety risks that may pose a significant risk to staff, (e.g. physical assault), service users and other relevant persons - are to be reported in accordance with the Trust's risk management strategy.

Specialist advice should be sought from the Security and Fire Officer regarding the identification of appropriate control measures to address significant, security risks.

6.2 Assessing Risks

Workplace risk assessments are to be undertaken and effectively managed in accordance with the Trust's *Risk Management Strategy* and supporting documents.

6.3 Risk Management and Action Plans

Workplace risk assessments and action plans devised to mitigate risk are to be made readily available, upon request by any relevant person(s).

Where deemed appropriate, crime prevention partnerships - with an interest in security within the NHS - will be established with external organisations, including the Police and other agencies.

6.4 Risk Review

A review of the control measures, identified within a risk assessment, is to be undertaken following reported incidents or changes to workplace processes with a view to ensure they remain suitable and sufficient to mitigate identified risks, so far as reasonably possible.

6.5 **Reporting Incidents and Serious Incidents**

The Trust has specific incident reporting arrangements, all security breaches and incidents as documented throughout this policy should be reported in accordance with the Trust *Incident Management Policy and Procedure (including Serious Incidents)*. All staff should be aware of and familiar with incident reporting arrangements.

6.6 **Protection of Staff - Tackling Aggression and Violence**

The Trust acknowledges that staff may be exposed to or involved directly in incidents of aggression or violence whilst providing healthcare services, incidents involving members of the public are not to be tolerated and reported to the Police whilst incidents involving service users will be investigated and assessed on an individual basis. Information on the management of aggression and violence is provided in Trust policy document: *Aggression and Violence - Respectful, Response and Reduction*.

In order to make a full assessment of whether an individual accused of offending should be arrested, charged or diverted from the criminal justice system, the Police are to be provided by the Trust with appropriate information on mentally vulnerable suspects to assist them in determining an appropriate course of action.

The Trust will undertake a training needs analysis to identify staff roles and responsibilities and provide suitable Conflict Resolution Training (CRT) to effectively manage potential incidents of workplace violence and aggression.

6.7 **Security and Management of Assets and Property**

The Trust will ensure that all staff, assets and property are suitably protected by means of physical, psychological and all other security measures as considered appropriate to achieve an identified aim. Responsibility for the security of staff, assets and property will be delegated to managers and staff in accordance with the Trust's policy document: *Scheme of Delegation*.

Managers with responsibility for work premises are to devise, record and bring to the attention of relevant staff any security arrangements with the purpose of providing a safe and secure environment.

The Trust will ensure, through its governance arrangements, that Trust assets and belongings, and those of service users for whom the Trust has responsibility, are suitably protected to prevent damage or loss from inappropriate actions or criminal activity.

The Director of Finance will, in accordance with the policy document: *Scheme of Delegation*, delegate powers to manage the approval of financial transactions initiated by other directorates across the Trust and prepare, document and maintain detailed financial procedures and systems incorporating the principles of separation of duties and internal checks to supplement instructions.

Directors of service, other directors and line managers have delegated responsibility to ensure all reasonable measures are undertaken to protect and secure the organisation's assets and property to prevent loss and/or damage.

Organisational assets valued at above £5,000 will be recorded on a Corporate Asset Register; departmental business critical assets valued below £5,000 will be recorded and held on a central register with suitable procedural arrangement developed to ensure the lifecycle of the asset is monitored from procurement to return, decommissioning and disposal.

6.8 **Investigations, Sanctions and Publication**

The Trust will investigate all reported incidents/offences committed against staff or organisational assets, the investigation officer will where considered necessary seek assistance from the Security Officer and/or the Police; incidents committed by members of the public are to be directed to the Police for investigation.

The Trust will where sanctions are taken against individuals give consideration to publicising sanctions in appropriate media with a view to deterring other potential offenders.

All staff have a 'duty of care' in accordance with Trust policy document: *Scheme of Delegation* to protect staff, Trust assets and property from the point of procurement to disposal. Managers are to devise suitable procedural arrangements, where considered necessary, to ensure assets are accounted for and property, for which they have responsibility, are appropriately secured and protected. Measures to deter, prevent and detect criminal activities are identified in Section 9.1 *Strategy*.

6.9 **Recovering Financial Losses**

The Trust will endeavour to recover any financial losses as a result of theft, damage to assets, property or premises etc. caused by criminal activity.

All such losses are to be reported by line management in submitting the relevant report forms in accordance with Trust policy document: *Incident Management Policy and Procedure (including Serious Incidents)* and the policy document: *Losses and Special Payments* to Directorate Nominees.

6.10 **Major Incident and Contingencies - Lockdown**

In the event of a major incident the Trust will implement its policy document: *Emergency Preparedness, Resilience and Recovery (EPRR) Responses to Major or Critical Incidents*; the outlines how the organisation will operate during a major incident. In the event the control of movement is required within a premise, a process known as lockdown will be implemented.

Lockdown is the controlling of movement, access and egress of people from, around or in to an area or premise in response to an identified risk, threat or hazard that might impact upon the security of staff, service users or visitors.

6.11 **Medicines, Drugs, Prescription Forms and Hazardous Materials**

The Trust will ensure all medicines are strictly controlled. Specific instructions to assist staff in the control and management of medicines are available in its policy document *Medicines Management*. Members of staff who are accountable and responsible for medicines, drugs and prescription forms are to be familiar with the policy requirements and implement identified security arrangements devised for medicine security.

6.12 **Counter-terrorism**

All staff should be constantly vigilant for the threat of terrorist activity. Terrorist activities range from overt acts, such as shootings, bombings and chemical attacks; they also take more subtle forms such as information gathering and blackmail.

Staff should be aware of suspect packages, un-attended items, the threat of bomb attacks and suspicious incidents, which are to be reported immediately to their line manager, building manager and the Trust's Security Officer.

Counter-terrorism and contingency planning will be undertaken within the Trust by its Security Management Director. External advice from security specialists, including the Counter-Terrorism Security Advisor (CTSA), employed by South Yorkshire Police, will be consulted as considered necessary to ensure the provision of protective and counter-terrorism measures are appropriate to the threat(s) posed to the Trust.

The Trust's Emergency Planning System will ensure terrorism risks are thoroughly evaluated and analysed so that appropriate, protective measures can be developed.

Improvised Explosive Devices (IEDs), Chemical, Biological and Radiological and Nuclear (CBRN) devices are often delivered in a variety of forms and could be considered as a suspicious package or object. Staff should be particularly aware of items, objects or devices which:

- Should not be there;
- Cannot be accounted for;
- Are out of place with its surroundings.

Where it is suspected that an IED has been identified, under no circumstances are members of staff to attempt to open it/them.

6.13 **Lone Working**

The Trust recognises that some members of staff will at times be required to work on their own, or away from their base location to undertake part of their duties. Effective managerial arrangements must be implemented to ensure, so far as reasonably practically possible, the security and wellbeing of lone workers in accordance with the Trust policy document: *Lone Worker*.

6.14 **Dangerous and 'Offensive' Weapons**

The term 'weapon' means any knife, or other type of sharply bladed or pointed object, or any object that could be used to threaten or injure another person. Any implement or object which could cause injury or harm may be considered to be a 'dangerous' weapon e.g. a chair, screwdriver or other similar objects, the carrying of such object is not an offence however; when brandished in a threatening manner it is considered to be an 'offensive' weapon, all such incidents involving offensive weapons are to be reported to the Police, 'Offensive' weapons are defined within the *Prevention of Crime Act (1953)* as ***'any article made or adapted for the use for causing injury to the person, or intended by the person having it with him for such use by him or by some other person'***.

Any weapon brought in to Trust premises by a service user(s) should be removed, stored temporarily in a secure place and the Trust's Security Officer notified immediately. The Security Officer will arrange for disposal via the Police.

It is acknowledged that some service users, (i.e. Sikhs), wish to carry a Kirpan; a ceremonial knife, as an act of religious obligation. After plenty of discussion and consideration it has been decided that it is un-acceptable for this to occur on Trust premises.

All items referred to as Kirpans will be treated in the same way as any other potentially dangerous or offensive weapon, as described above.

Some Kirpans are made so they allow the person to meet their religious obligation, but could not in any way qualify as dangerous or offensive. If this is deemed to be the case when the Police inspect the item then the Police will most likely decline removing it from the premises. In this instance, the Kirpan will be retained in safe-keeping until the service user leaves Trust premises and it is appropriate to return the item to them.

The Trust has to place the wellbeing of all its service users above that of any one individual, and the carrying of a 'harmless' Kirpan has the potential to confuse service users, and the public, as to the Trust's position on knives. It may even cause distress to a service user whose perception is altered due to confusion, or due to persecutory or paranoid ideation.

7. **Dissemination, Storage and Archiving (Control)**

Within 5 working days of ratification of this policy, an 'All SHSC staff' email alert will be sent to staff, informing them of the new/revised policy and attaching the link showing where the policy can be accessed via the intranet and internet. In addition, Clinical, Service and Support Directors will be instructed to ensure that all teams and areas are made aware of this new/revised policy and how to apply it.

The previous Security Policy, (version 6), will be removed from the Trust intranet and internet by the Director of Corporate Governance and archived on the policy database. Team managers are responsible for ensuring it is also removed from any policy and procedure manuals or files stored in their offices and destroyed. A dissemination record, (see Appendix B), will be created by the Policy Lead.

8. **Training and Other Resource Implications**

Security Awareness Training is to be an integral part of organisational training and education in accordance with the Trust's *Risk Management Strategy*.

Line managers are to undertake a staff training needs analysis and give consideration to the type and frequency of training required; this may include:

- SHSC corporate induction
- Local workplace induction
- Individual/personal safety awareness based on job description and risk assessment
- Use and maintenance of security equipment
- Security protocols/procedures for the workplace, including the rationale behind the protocols
- Management of situations of potential or actual abuse, aggression or violence, including:
 - understanding the causes
 - recognising the warning signs
 - identifying when and where to get assistance
 - interpersonal skills/defusing techniques

Managers and staff must refer to the Trust's policy *Aggression and Violence: Respectful Response and Reduction* for detailed information.

9. **Audit, Monitoring and Review**

Line managers are to undertake an internal audit of workplace security arrangements to ensure they remain 'fit for purpose'. Managers must maintain appropriate records of workplace safe systems of work, procedural arrangements, risk assessments and demonstrate staff awareness of the policy, which should be reviewed annually, or as considered appropriate.

The Security and Fire Officer will monitor and review the policy as and when required, every three years or following legislative and NHS requirements.

10. Implementation Plan

Action/Task	Responsible Person	Deadline	Progress update
Draft, revised policy submitted to the Health and Safety Group and Service Directors for Consultation	Security and Fire Officer		
Final Draft sent to the Policy Governance Group	Security and Fire Officer		
Final Draft sent to the Quality Assurance Committee	Chair of Policy Governance Group		
Final Draft sent to the Executive Directors' Group for Ratification	Chair of Quality Assurance Committee		
Policy approved by the Executive Directors' Group	Chair of Executive Directors Group		
Policy placed on the Trust's intranet and internet for dissemination; all previous versions to be removed with email alert to all staff	Head of Communications		
Managers to inform staff for which they have responsibility of the revised Policy	Managers		

11. Links to Other Policies, Standards and Legislation

This policy meets various legislative requirements and is necessary to demonstrate compliance with the:

- SHSC Policy: Health and Safety
- SHSC Policy: Standing Orders, Reservations and Delegation of Powers and Standing Financial Instructions
- SHSC Policy: Scheme of Delegation
- SHSC Policy: Medicines Management
- SHSC's: Risk Management Strategy
- SHSC Policy: Incident Management Policy and Procedure (including Serious Incidents)
- SHSC Policy: Aggression and Violence- Respectful, Response and Reduction
- SHSC Policy: Emergency Preparedness, Resilience and Recovery (EPRR) Responses to Major or Critical Incidents
- SHSC Policy: Lone Worker
- SHSC Policy: Fraud, Bribery and Corruption
- SHSC Policy on Policies, which require an **Equality Impact Assessment Form, Human Rights Act Assessment Checklist** and a **Development and Consultation Process: see Supplementary Sections.**

12. Contact Details

Title	Name	Phone	E-mail
Security Management Director (Executive Director of Finance)	Phillip Easthope	30 50765	phillip.easthope@shsc.nhs.uk
Security and Fire Officer	Stephen Price	27 18189	stephen.price@shsc.nhs.uk

13. References

The contents of this policy guidance were taken from the following key references:

- Health and Safety at Work Act 1974
- Prevention of Crime Act 1953
- Management of Health and Safety at Work Regulations 1999

Appendix A - Version Control and Amendment Log

Version No.	Type of Change	Date	Description of Change(s)
7	Review	July 2018	<p>Amendments to Sections 5 (<i>Duties</i>) and 6 (<i>Processes</i>).</p> <p>Removal of attached procedural instructions, namely:</p> <ul style="list-style-type: none"> • Security Assessment Check Sheet • Tackling Violence and Anti-Social Behaviour • Lockdown • Improvised Explosive Devices (IEDs) and Similar Threats • Offensive Weapons <p>6.5 - <i>Reporting Incidents and Serious Untoward Incidents</i> changed to <i>Reporting Incidents and Serious Incidents</i>.</p>

Appendix B - Dissemination Record

Version	Date on website - (intranet and internet)	Date of 'all SHSC staff' email	Any other promotion/ dissemination, (include dates)
7	January 2019	January 2019	N/A

Appendix C - Equality Impact Assessment Form

Equality Impact Assessment Process for Policies Developed Under the Policy on Policies

Stage 1 - Complete draft policy

Stage 2 - Relevance - is the policy potentially relevant to equality, i.e. will this policy potentially impact on staff, patients or the public? If **NO**, no further action is required. Please sign and date the following statement. If **YES**, proceed to Stage 3

This policy does not impact on staff, service users or the public (insert name and date)

Stephen Price, September 2018

Stage 3 - Policy screening - public authorities are legally required to have 'due regard' to eliminating discrimination, advancing equal opportunity and fostering good relations, in relation to people who share certain 'protected characteristics' and those that do not. The following table should be used to consider this and inform changes to the policy (indicate yes/no/ don't know and note reasons). Please see the SHSC guidance on equality impact assessment for examples and detailed advice; this can be found at <http://www.shsc.nhs.uk/about-us/equality--human-rights>

	Does any aspect of this policy actually or potentially discriminate against this group?	Can equality of opportunity for this group be improved through this policy or changes to this policy?	Can this policy be amended so that it works to enhance relations between people in this group and people not in this group?
AGE	No		
DISABILITY	No		
GENDER REASSIGNMENT	No		
PREGNANCY AND MATERNITY	No		
RACE	No		
RELIGION OR BELIEF	No		
SEX	No		
SEXUAL ORIENTATION	No		
MARRIAGE AND CIVIL PARTNERSHIP	No		

Security Policy
page 16 of 28

Stage 4 - Policy Revision - Make amendments to the policy or identify any remedial action required (action should be noted in the policy implementation plan section)

Please delete as appropriate: Policy Amended/Action Identified/No Changes Made

Impact Assessment Completed by (insert name and date)

Stephen Price, September 2018

Security Policy
page 16 of 23

Appendix D - Human Rights Act Assessment Checklist

You need to be confident that no aspect of this policy breaches a person's Human Rights. You can assume that if a policy is directly based on a law or national policy it will not therefore breach Human Rights.

If the policy, or any procedure(s) in the policy, is based on a local decision which impacts on individuals, there is a need to ensure their human rights are not breached. To do this, refer to the more detailed guidance that is available on the SHSC website - <http://www.justice.gov.uk/downloads/human-rights/act-studyguide.pdf> (relevant sections numbers are referenced in grey boxes on diagram) and work through the flow chart on the next page.

1. Is your policy based on, and in-line with, the current law, (including case law), or policy?

Yes. No further action needed

No. Work through the flow diagram over the page then answer questions 2 and 3 below

2. On completion of flow diagram, is further action needed?

No. No further action needed

Yes, go to question 3

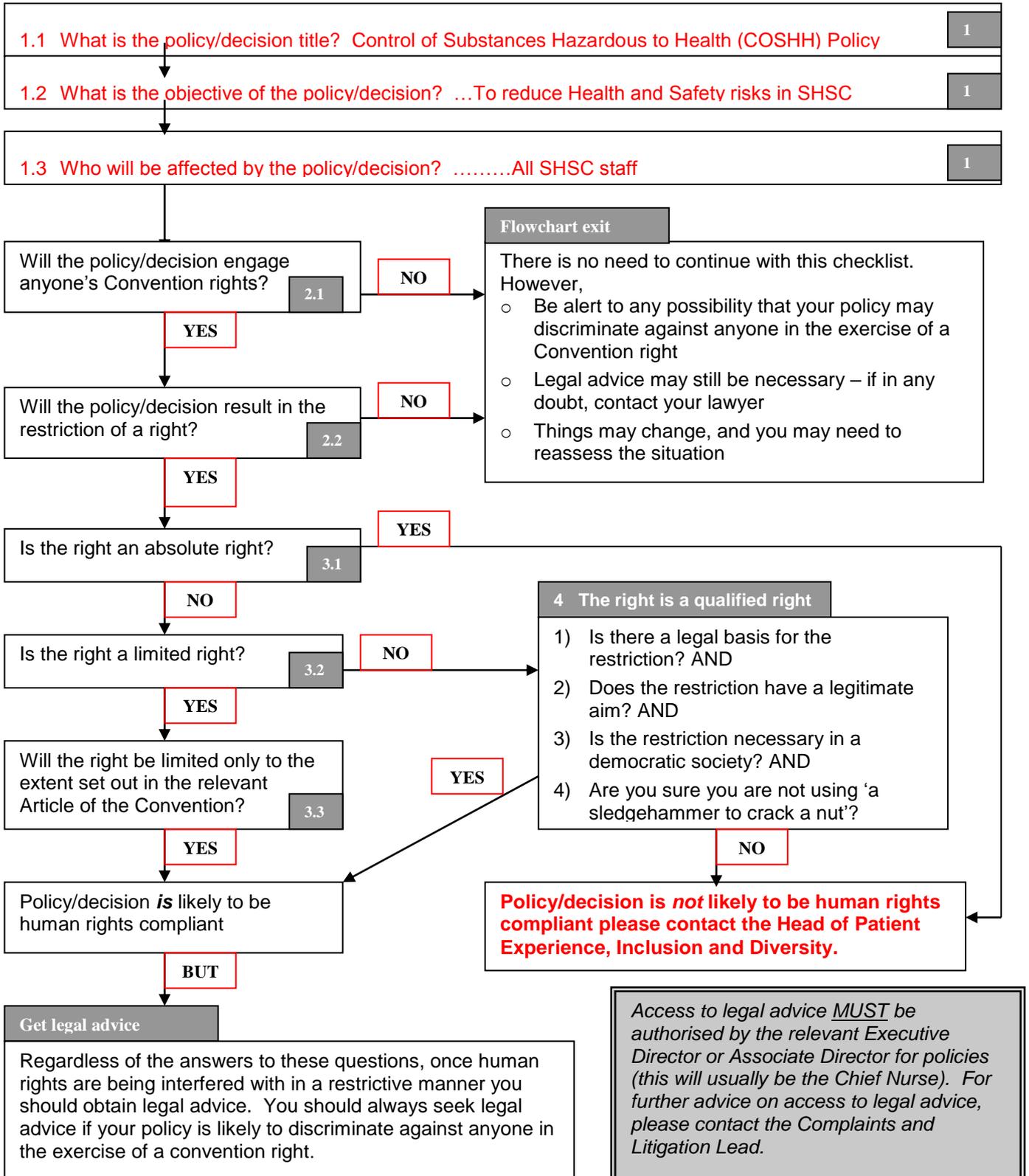
3. **Complete the table below to provide details of the actions required**

Action required	By what date	Responsible person

Human Rights Assessment Flow Chart

Complete text answers in boxes 1.1 - 1.3 and highlight your path through the flowchart by filling the YES/NO boxes red (do this by clicking on the YES/NO text boxes and then from the Format menu on the toolbar, choose 'Format Text Box' and choose red from the Fill colour option).

Once the flowchart is completed, return to the previous page to complete the Human Rights Act Assessment Form.



Appendix E - Development, Consultation and Verification Record

Name of Policy: Security		Name of Policy Lead: Stephen Price	
Date: December 2018		Contact Details: (0114) 27 18189	
Consultation Plan:			
Health and Safety Group			
Directors of Corporate Functions			
Service Directors			
Quality and Assurance Committee			
Executive Director of Finance			
Emergency Planning Manager			
Staff-side Representatives			
RECORD OF CONSULTATION (interactive)			
Group or individual consulted	Date of consultation/ response received	Comments on draft policy	Your response (say if policy amended - if not, why not)
Policy Governance Group (PGG)	November 2018	The flowchart was requested to be altered. The rationale was not stated and no further information given.	Not actioned.
Emergency Planning Manager	August 2018	Section 5 Duties - <i>Emergency Planning Manager</i> . Amended in-line with the Emergency Planning Manager's comments	Policy amended
Health and Safety Group	August 2018	Section 5 Duties - <i>Chief Pharmacist</i> . Amended in-line with the Deputy Director of Pharmacy Services' comments	Policy amended

Group or individual consulted	Date of consultation/ response received	Comments on draft policy	Your response (say if policy amended - if not, why not)
Policy Governance Group (PGG)	August 2018	Section 5 Duties: Advised to include job roles for the Clinical and Service Directors and the Directors of Corporate Functions	Not actioned. Job roles/titles frequently change to reflect service requirements. Instead, the matter is collectively addressed in the section headed <i>Managers</i> (in Section 5: <i>Duties</i>)
Policy Governance Group (PGG)	November 2018	Section 6.5 - <i>Reporting Incidents and Serious Untoward Incidents.</i> Advised to change the heading and content to <i>Reporting Incidents and Serious Incidents.</i>	Policy amended
Staff-side	August 2018	Section 6.12 <i>Counter-terrorism:</i> The wording ' <i>NHS hospitals and healthcare premises are not normally the targets of terrorist activists</i> ' has been removed	Policy amended
Staff-side	September 2018	Section 6.14 <i>Dangerous and 'Offensive' Weapons:</i> The addition of 3 paragraphs re Kirpans/Sikhs *	Policy amended
Policy Governance Group (PGG)	11 July 2018	Section 11 <i>Links to Other Policies, Standards and Legislation:</i> Removal of text reference to fraud, bribery and corruption and insert reference to policy	Policy amended

Group or individual consulted	Date of consultation/ response received	Comments on draft policy	Your response (say if policy amended - if not, why not)
Staff-side	August 2018	Appendix C <i>Equality Impact Assessment</i> . Staff-side indicated the policy discriminated against religion or belief and should read Yes	Policy amended so as not to discriminate against religion or belief. See Section 6.14 above referring to Kirpans/Sikhs *
Staff-side	August 2018	Appendix C <i>Equality Impact Assessment</i> . Amended to include the protected characteristic for the EIA, which is Marriage and Civil Partnership	Policy amended
Policy Governance Group (PGG)	August 2018	Advised to add the <i>VIP/ Celebrity Visits</i> Standard Operating Procedure as an appendix	Not actioned. Standard Operating Procedures will not be incorporated in to the policy. Procedural arrangements should be stand-alone documents referencing policy amendments, (following changes to the workplace and reported incidents), without having to amend the policy.

Appendix F - Policy Checklist

Please use this as a checklist for policy completion. The style and format of policies should follow the policy template, which can be downloaded from the intranet.

1. Cover sheet



All policies must have a cover sheet which includes:

- The Trust name and logo ✓
- The title of the policy (in large font size as detailed in the template) ✓
- Executive or Associate Director lead for the policy ✓
- The policy author and lead ✓
- The implementation lead (to receive feedback on the implementation) ✓
- Date of initial draft policy ✓
- Date of consultation ✓
- Date of verification ✓
- Date of ratification ✓
- Date of issue ✓
- Ratifying body ✓
- Date for review ✓
- Target audience ✓
- Document type ✓
- Document status ✓
- Keywords ✓
- Policy version and advice on availability and storage ✓

2. Contents page



3. Flowchart



4. Introduction



5. Scope



6. Definitions



7. Purpose



8. Duties



9. Process



10. Dissemination, storage and archiving (control)



11. Training and other resource implications



12. Audit, monitoring and review

This section should describe how the implementation and impact of the policy will be monitored and audited and when it will be reviewed. It should include timescales and frequency of audits. It must include the monitoring template as shown in the policy template (example below).



Monitoring Compliance Template						
Minimum requirement	Process for monitoring	Responsible individual/group/committee	Frequency of monitoring	Review of results process, (e.g. who does this?)	Responsible individual/group/committee for action plan development	Responsible individual/group/committee for action plan monitoring and implementation
A) describe which aspect this is monitoring?	e.g. review, audit	e.g. Education and Training Steering Group	e.g. annual	e.g. Quality Assurance Committee	e.g. Education and Training Steering Group	e.g. Quality Assurance Committee

13. Implementation plan



14. Links to other policies (associated documents)



15. Contact details



16. References



17. Version control and amendment log - (Appendix A)



18. Dissemination Record - (Appendix B)



19. Equality Impact Assessment Form - (Appendix C)



20. Human Rights Act Assessment Checklist - (Appendix D)



21. Policy development and consultation process - (Appendix E)



22. Policy Checklist - (Appendix F)

